NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755

STAT

3 May 1982

Mr. Sloan
Director of Operations
Defense Audiovisual Agency
Norton AFB, CA 92409

Dear Mr. Sloan:

The DoD Computer Security Center (CSC) and the DCI Security Awareness Working Group are sponsoring a program to promote the role of the CSC and to assure a sense of security awareness and individual responsibility of appropriate Government and industry personnel to the realities of computer security, security products relating to ADP functions, and security vulnerabilities of computer systems.

We would like this program (see attached scope and objectives) to be formed around a video tape series produced by a contracted production company (professional script, actors, etc). The CSC and the DCI Working Group have FY82 funds for this project and would like to obligate those funds as soon as possible. Therefore, a timely response to our requirements from you would be appreciated.

The DoD CSC will provide technical expertise and technical consultants to assist in all phases of the program. In order to minimize TDY and travel costs, we would like the development and production of the program to be done within the Washington, DC, Ft. George G. Meade, MD area if at all possible.

Sincerely,

MELVILLE H. KLEIN
Director
DoD Computer Security Center

SCOPE:

Three video programs are proposed. A primary program, 20-25 minutes long, and two optional programs, 15-20 minutes long. The first program shall be a general overview to meet the objectives below.

AUDIENCE:

Government and industrial personnel engaged in the management, design, development, procurement, operation, or security of computer systems.

CLASSIFICATION:

The primary program to be unclassified.

Government and contract personnel involved in producing these programs should possess SECRET NOFORN clearances for access to this level of information for background research purposes.

OBJECTIVES OF THE PRIMARY PROGRAM:

1. To describe the mission and function of the DoD Computer Security Center (CSC) and define its authority in a tactful way.

2. To outline the CSC's role in providing guidance in the area of computer security as directed by its charter and to assist the community at large in addressing their computer security problems. An image of helpfulness and availability should be promoted.

3. To assure a keen sense of individual responsibilities for awareness and correction of security vulnerabilities in computer systems and security software products.

4. Present examples of how technical shortcomings of computer software and hardware resulted in computer exploitation, crime, and denial of services.

5. To present the unique contributions of the CSC to the community in the areas of research and development, assistance in the acquisition of DoD computer systems, dissemination of computer security information, and evaluation of commercial computer security products. Again, the image conveyed is very important.

6. Describe the different operating modes (multilevel, systems high, etc.) for computer systems and the vulnerabilities associated with these modes.

OBJECTIVES OF OPTIONAL PROGRAMS:

1. To provide sufficient knowledge of ADP security so that ADP personnel do not, through ignorance or accident, introduce computer security vulnerabilities.

2. To describe a trusted computer system, its components and its purpose, and enable ADP personnel to recognize when such a system should be applied.

3. To explain the vulnerability issues of a trusted computer base (multilevel, security classification, user identification).

4. To compare how data on trusted and non-trusted systems can be manipulated by both authorized and unauthorized users.

5. To demonstrate the need for explicitly labeling internal computer data.

6. To illustrate the difference between handling labeled data in a hard copy (printed) environment, and handling the same data when it is stored and/or manipulated within a computer system (memory, disk·fiber, etc).

7. To show that a trusted computer system complies with DoD Directive 5200.1R, dated 17 October 1980; titled Information Security Program Regulation.

8. To create an awareness of subversive vulnerabilities on computer systems currently in use. Explain the terms "Trojan horse" and "Trap door", and demonstrate how subversion takes place on these systems.

9. To create an awareness of penetration vulnerabilities on non-trusted computer systems, demonstrate penetration techniques, and demonstrate the existence of penetration holes in a system, despite the lack of evidence pointing to actual penetration. ADP personnel should be aware that fixes of penetration holes do not assure that all holes have been found, and that often fixes create new penetration holes.

10. To create an awareness of security vulnerabilities of computer networks and how these networks can be exploited.

11. To show that each Trusted system within a computer network must "understand" the "Trustworthiness" of the other systems in the network.

12. To demonstrate the importance of labeling all data to ensure that each connected system will "know" how to handle that data within the network.

13. To identify the principal tools used to prevent subversion and penetration (data labeling and user identification) of computer systems.